

w1384

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-358706
(43)Date of publication of application : 26.12.2001

(51)Int.Cl. H04L 9/08
G06F 12/00
G06F 12/14
G06F 17/60

(21)Application number : 2001-106539 (71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(22)Date of filing : 04.04.2001 (72)Inventor : SHIBATA OSAMU
SEKIBE TSUTOMU

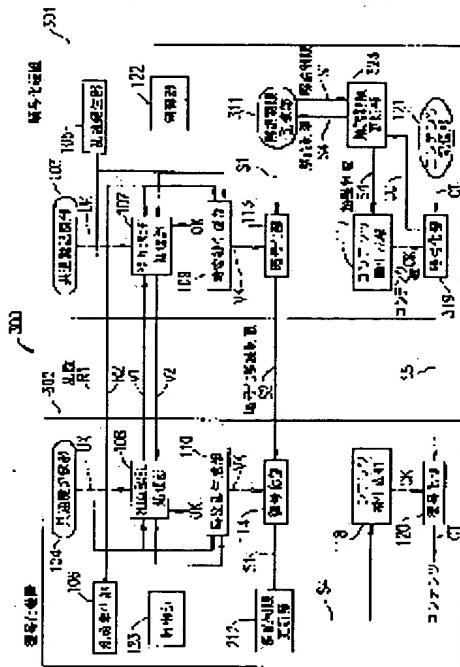
(30)Priority
Priority number : 2000105525 Priority date : 06.04.2000 Priority country : JP

(54) COPYRIGHT PROTECTION SYSTEM, ENCIPHERING DEVICE, DECODING DEVICE AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a system for preventing illegal decoding of digital contents which are recorded on a recording medium and have decoding limit.

SOLUTION: In a communication system consisting of an enciphering device and a decoding device which share a contents key perform cipher communication by using the contents key, the enciphering device and the decoding device mutually authenticate that the opposite devices are a legitimate device with mutual authentication and also share a time varying key form a random number used for the mutual authentication. The decoding limit such as the number of reproducing times data stored in the decoding device is enciphered with the time varying key, transferred to the decoding device while security is conducted, also updated by both devices and the decoding limit is shared. In the case of loading contents, the cipher communication is performed by using a contents key generated from the updated decoding limitation.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2001-358706
(P2001-358706A)

(43)公開日 平成13年12月26日 (2001.12.26)

(51) Int.Cl. ⁷	識別記号	F I	テマコード(参考)
H 04 L 9/08		G 06 F 12/00	5 3 7 H 5 B 0 1 7
G 06 F 12/00	5 3 7	12/14	3 2 0 A 5 B 0 8 2
12/14	3 2 0		3 2 0 F 5 J 1 0 4
17/60	1 4 2	17/60	1 4 2
			3 0 2 E

審査請求 未請求 請求項の数47 OL (全18頁) 最終頁に続く

(21)出願番号	特願2001-106539(P2001-106539)
(22)出願日	平成13年4月4日 (2001.4.4)
(31)優先権主張番号	特願2000-105525(P2000-105525)
(32)優先日	平成12年4月6日 (2000.4.6)
(33)優先権主張国	日本 (JP)

(71)出願人	000005821 松下電器産業株式会社 大阪府門真市大字門真1006番地
(72)発明者	柴田 修 大阪府門真市大字門真1006番地 松下電器 産業株式会社内
(72)発明者	関部 勉 大阪府門真市大字門真1006番地 松下電器 産業株式会社内
(74)代理人	100078282 弁理士 山本 秀策

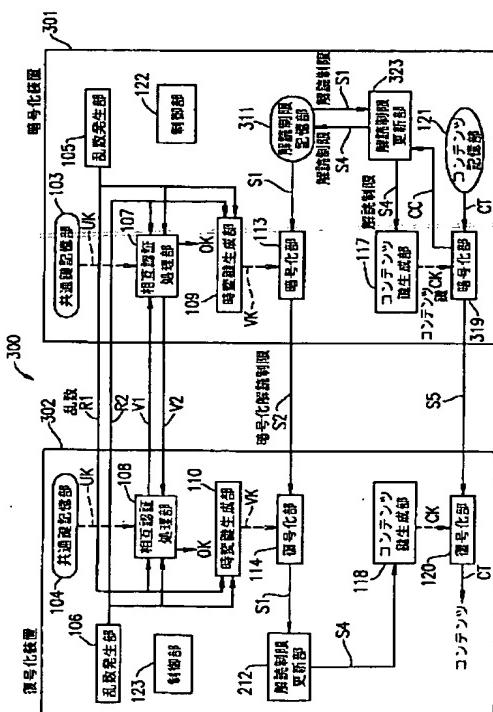
最終頁に続く

(54)【発明の名称】著作物保護システム、暗号化装置、復号化装置および記録媒体

(57)【要約】

【課題】 記録媒体に記録された解読制限を持ったディジタルコンテンツの不正解読を防止するシステムを提供する。

【解決手段】 コンテンツ鍵の共有化とそのコンテンツ鍵を用いた暗号通信を行う暗号化装置および復号化装置から構成される通信システムにおいて、暗号化装置及び復号化装置は相互認証によって相手機器が正当な機器であることを認証し合い、かつ相互認証に用いた乱数から時変鍵を共有化する。復号化装置に格納されている再生回数データなどの解読制限を時変鍵で暗号化し、機密保護した状態で暗号化装置に転送し、かつ両機器において解読制限の更新を行い解読制限を共有化する。コンテンツのロードに際しては、更新された解読制限から生成したコンテンツ鍵を用いて暗号通信を行う構成とした。



【特許請求の範囲】

【請求項1】 コンテンツ鍵を用いて暗号通信を行う暗号化装置および復号化装置から構成される著作物保護システムであって、

前記暗号化装置は、コンテンツを記憶するコンテンツ記憶手段と、

第1解読制限を更新して得られる第2解読制限に基づいて前記コンテンツ鍵を生成する第1コンテンツ鍵生成手段と、

前記コンテンツを前記コンテンツ鍵に基づいて暗号化し、暗号化コンテンツを出力する第1暗号化手段とを具備し、

前記復号化装置は、前記第2解読制限から前記コンテンツ鍵を生成する第2コンテンツ鍵生成手段と、

前記暗号化コンテンツを前記第2コンテンツ鍵生成手段により生成された前記コンテンツ鍵を用いて復号化する第1復号化手段とを具備することを特徴とする著作物保護システム。

【請求項2】 前記復号化装置は、前記第1解読制限を解読制限更新則に基づいて前記第2解読制限に更新する解読制限更新手段と、

前記第2解読制限を時変鍵に基づいて暗号化し、第1暗号化解読制限を出力する第2暗号化手段とをさらに具備し、

前記暗号化装置は、前記第2暗号化手段から転送される前記第1暗号化解読制限を前記時変鍵に基づいて復号化し、前記第2解読制限を生成する第2復号化手段をさらに具備し、

前記第1コンテンツ鍵生成手段は、前記第2復号化手段により生成された前記第2解読制限に基づいて前記コンテンツ鍵を生成する、請求項1記載の著作物保護システム。

【請求項3】 前記暗号化装置は、共通鍵を記憶する第1共通鍵記憶手段と、

前記第1解読制限を記憶する解読制限記憶手段と、

第1乱数を生成する第1乱数発生手段と、

前記第1乱数と前記復号化装置から転送される第2乱数とを用いて前記復号化装置と相互認証処理を行なう第1相互認証処理手段と、

前記第1相互認証処理手段における認証受理をうけて前記第1乱数と前記第2乱数とから前記時変鍵を生成する第1時変鍵生成手段と、

前記第1解読制限を前記時変鍵を用いて暗号化して第2暗号化解読制限を出力する第3暗号化手段とをさらに具備し、

前記復号化装置は、前記共通鍵を記憶する第2共通鍵記憶手段と、

前記第2乱数を生成する第2乱数発生手段と、

前記第2乱数と前記第1乱数とを用いて前記暗号化装置と相互認証を行なう第2相互認証処理手段と、

前記第2相互認証処理手段における認証受理をうけて前記第2乱数と前記第1乱数とから前記時変鍵を生成する第2時変鍵生成手段と、

前記第2暗号化解読制限を前記時変鍵を用いて復号化する第3復号化手段とさらに具備する、請求項2記載の著作物保護システム。

【請求項4】 前記復号化装置は、前記第1解読制限を解読制限更新則に基づいて第2解読制限に更新する第1解読制限更新手段をさらに具備し、

前記第2コンテンツ鍵生成手段は、前記第1解読制限更新手段により更新された前記第2解読制限に基づいて前記コンテンツ鍵を生成し、

前記暗号化装置は、前記復号化装置の第1解読制限更新手段における解読制限の更新をうけて、前記第1解読制限を解読制限更新則に従って前記第2解読制限に更新する第2解読制限更新手段をさらに具備し、

前記第1コンテンツ鍵生成手段は、前記第1解読制限更新手段により更新された前記第2解読制限に基づいて前記コンテンツ鍵を生成する、請求項1記載の著作物保護システム。

【請求項5】 前記暗号化装置は、前記共通鍵を記憶する第1共通鍵記憶手段と、

前記第1解読制限を記憶する解読制限記憶手段と、

第1乱数を生成する第1乱数発生手段と、

前記第1乱数と前記復号化装置から転送される第2乱数とを用いて前記復号化装置と相互認証を行なう第1相互認証処理手段と、

前記第1相互認証処理手段における認証受理をうけて前記第1乱数と前記第2乱数とから時変鍵を生成する第1時変鍵生成手段と、

前記第1解読制限を前記時変鍵を用いて暗号化して暗号化解読制限を出力する第2暗号化手段とをさらに具備し、

前記復号化装置は、前記共通鍵を記憶する第2共通鍵記憶手段と、

前記第2乱数を生成する第2乱数発生手段と、

前記第2乱数と前記第1乱数とを用いて前記暗号化装置と相互認証を行なう第2相互認証処理手段と、

前記第2相互認証処理手段における認証受理をうけて前記第2乱数と前記第1乱数とから前記時変鍵を生成する第2時変鍵生成手段と、

前記暗号化解読制限を前記時変鍵を用いて復号化する第2復号化手段とをさらに具備する、請求項4記載の著作物保護システム。

【請求項6】 前記第2解読制限更新手段は、予め前記第1解読制限を第2解読制限に更新し、

前記第2解読制限更新手段は、前記第1コンテンツ鍵生成手段に更新された前記第2解読制限を出力し、

前記第1コンテンツ鍵生成手段は、前記第2解読制限から前記コンテンツ鍵を生成し、

前記第2解読制限更新手段は、前記第1暗号化手段の処理が開始されたことをうけて、前記解読制限記憶手段に前記第2解読制限を格納する、請求項5記載の著作物保護システム。

【請求項7】 前記第1および第2時変鍵生成手段は、前記第1および第2乱数と前記共通鍵に基づいて前記時変鍵を生成する、請求項3記載の著作物保護システム。

【請求項8】 前記第1および第2コンテンツ鍵生成手段は、前記第2解読制限と前記時変鍵とに基づいて前記コンテンツ鍵を生成する、請求項3記載の著作物保護システム。

【請求項9】 前記暗号化装置および前記復号化装置は、前記暗号化装置および前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成する第1および第2データ系列鍵生成手段をそれぞれさらに具備し、前記第1および第2時変鍵生成手段は、前記第1および第2乱数と前記データ系列鍵とに基づいて前記時変鍵を生成する、請求項3記載の著作物保護システム。

【請求項10】 前記暗号化装置および前記復号化装置は、前記暗号化装置および前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成する第1および第2データ系列鍵生成手段をそれぞれさらに具備し、前記第1および第2時変鍵生成手段は、前記第1および第2乱数と前記共通鍵と前記データ系列鍵とに基づいて前記時変鍵を生成する、請求項3記載の著作物保護システム。

【請求項11】 前記暗号化装置および前記復号化装置は、前記暗号化装置および前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成する第1および第2データ系列鍵生成手段をそれぞれさらに具備し、前記第1および第2コンテンツ鍵生成手段は、前記第2解読制限と前記データ系列鍵とに基づいて前記コンテンツ生成鍵を生成する、請求項3記載の著作物保護システム。

【請求項12】 前記暗号化装置および前記復号化装置は、前記暗号化装置および前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成する第1および第2データ系列鍵生成手段をそれぞれさらに具備し、前記第1および第2コンテンツ鍵生成手段は、前記第2解読制限と前記時変鍵と前記データ系列鍵とに基づいて前記コンテンツ生成鍵を生成する、請求項3記載の著作物保護システム。

【請求項13】 前記第1および第2相互認証処理手段は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に相手機器が正当な機器であることを認証する、請求項3記載の著作物保護システム。

【請求項14】 コンテンツ鍵を用いて復号化装置と暗号通信を行う暗号化装置であって、前記暗号化装置は、コンテンツを記憶するコンテンツ記憶手段と、

第1解読制限を更新して得られる第2解読制限に基づいて前記コンテンツ鍵を生成するコンテンツ鍵生成手段と、

前記コンテンツを前記コンテンツ鍵に基づいて暗号化し、暗号化コンテンツを出力する第1暗号化手段とを具備することを特徴とする暗号化装置。

【請求項15】 前記暗号化装置は、前記復号化装置から転送される第1暗号化解読制限を時変鍵に基づいて復号化し、前記第2解読制限を生成する復号化手段をさらに具備し、

前記コンテンツ鍵生成手段は、前記復号化手段により生成された前記第2解読制限に基づいて前記コンテンツ鍵を生成する、請求項14記載の暗号化装置。

【請求項16】 前記暗号化装置は、共通鍵を記憶する共通鍵記憶手段と、

前記第1解読制限を記憶する解読制限記憶手段と、第1乱数を生成する第1乱数発生手段と、

前記第1乱数と前記復号化装置から転送される第2乱数とを用いて前記復号化装置と相互認証処理を行なう相互認証処理手段と、

前記相互認証処理手段における認証受理をうけて前記第1乱数と前記第2乱数とから前記時変鍵を生成する時変鍵生成手段と、

前記第1解読制限を前記時変鍵を用いて暗号化して第2暗号化解読制限を出力する第2暗号化手段とをさらに具備する、請求項15記載の暗号化装置。

【請求項17】 前記暗号化装置は、前記復号化装置の解読制限の更新をうけて、前記第1解読制限を解読制限更新則に従って前記第2解読制限に更新する解読制限更新手段をさらに具備し、

前記コンテンツ鍵生成手段は、前記解読制限更新手段により更新された前記第2解読制限に基づいて前記コンテンツ鍵を生成する、請求項14記載の暗号化装置。

【請求項18】 前記暗号化装置は、前記共通鍵を記憶する共通鍵記憶手段と、

前記第1解読制限を記憶する解読制限記憶手段と、第1乱数を生成する第1乱数発生手段と、

前記第1乱数と前記復号化装置から転送される第2乱数とを用いて前記復号化装置と相互認証を行なう相互認証処理手段と、

前記相互認証処理手段における認証受理をうけて前記第1乱数と前記第2乱数とから時変鍵を生成する時変鍵生成手段と、

前記第1解読制限を前記時変鍵を用いて暗号化して暗号化解読制限を出力する第2暗号化手段とをさらに具備する、請求項17記載の暗号化装置。

【請求項19】 前記解読制限更新手段は、予め前記第1解読制限を第2解読制限に更新し、

前記解読制限更新手段は、前記コンテンツ鍵生成手段に更新された前記第2解読制限を出力し、

前記コンテンツ鍵生成手段は、前記第2解読制限から前記コンテンツ鍵を生成し、

前記解読制限更新手段は、前記第1暗号化手段の処理が開始されたことをうけて、前記解読制限記憶手段に前記第2解読制限を格納する、請求項17記載の暗号化装置。

【請求項20】 前記時変鍵生成手段は、前記第1および第2乱数と前記共通鍵に基づいて前記時変鍵を生成する、請求項16記載の暗号化装置。

【請求項21】 前記コンテンツ鍵生成手段は、前記第2解読制限と前記時変鍵とに基づいて前記コンテンツ鍵を生成する、請求項16記載の暗号化装置。

【請求項22】 前記暗号化装置は、前記暗号化装置の出入力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、

前記時変鍵生成手段は、前記第1および第2乱数と前記データ系列鍵とに基づいて前記時変鍵を生成する、請求項16記載の暗号化装置。

【請求項23】 前記暗号化装置は、前記暗号化装置の出入力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、

前記時変鍵生成手段は、前記第1および第2乱数と前記共通鍵と前記データ系列鍵とに基づいて前記時変鍵を生成する、請求項16記載の暗号化装置。

【請求項24】 前記暗号化装置は、前記暗号化装置の出入力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、

前記コンテンツ鍵生成手段は、前記第2解読制限と前記データ系列鍵とに基づいて前記コンテンツ生成鍵を生成する、請求項16記載の暗号化装置。

【請求項25】 前記暗号化装置は、前記暗号化装置の出入力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、

前記コンテンツ鍵生成手段は、前記第2解読制限と前記時変鍵と前記データ系列鍵とに基づいて前記コンテンツ生成鍵を生成する、請求項16記載の暗号化装置。

【請求項26】 コンテンツ鍵を用いて暗号化装置と暗号通信を行う復号化装置であって、

前記復号化装置は、第2解読制限から前記コンテンツ鍵を生成するコンテンツ鍵生成手段と、

暗号化コンテンツを前記コンテンツ鍵生成手段により生成された前記コンテンツ鍵を用いて復号化する第1復号化手段とを具備することを特徴とする復号化装置。

【請求項27】 前記復号化装置は、前記第1解読制限を解読制限更新則に基づいて前記第2解読制限に更新する解読制限更新手段と、

前記第2解読制限を時変鍵に基づいて暗号化し、第1暗号化解読制限を出力する暗号化手段とをさらに具備する、請求項26記載の復号化装置。

【請求項28】 前記復号化装置は、前記共通鍵を記憶

する共通鍵記憶手段と、

前記第2乱数を生成する乱数発生手段と、

前記第2乱数と第1乱数とを用いて前記暗号化装置と相互認証を行なう相互認証処理手段と、

前記相互認証処理手段における認証受理をうけて前記第2乱数と前記第1乱数とから前記時変鍵を生成する時変鍵生成手段と、

第1暗号化解読制限を前記時変鍵を用いて復号化する第2復号化手段とをさらに備える、請求項27記載の復号化装置。

【請求項29】 前記復号化装置は、前記第1解読制限を解読制限更新則に基づいて第2解読制限に更新する解読制限更新手段をさらに備え、

前記コンテンツ鍵生成手段は、前記解読制限更新手段により更新された前記第2解読制限に基づいて前記コンテンツ鍵を生成する、請求項26記載の復号化装置。

【請求項30】 前記復号化装置は、前記共通鍵を記憶する第2共通鍵記憶手段と、

前記第2乱数を生成する第2乱数発生手段と、

前記第2乱数と第1乱数とを用いて前記暗号化装置と相互認証を行なう相互認証処理手段と、

前記相互認証処理手段における認証受理をうけて前記第2乱数と前記第1乱数とから前記時変鍵を生成する時変鍵生成手段と、

暗号化解読制限を前記時変鍵を用いて復号化する第2復号化手段とをさらに具備する、請求項29記載の復号化装置。

【請求項31】 前記時変鍵生成手段は、前記第1および第2乱数と前記共通鍵に基づいて前記時変鍵を生成する、請求項28記載の復号化装置。

【請求項32】 前記コンテンツ鍵生成手段は、前記第2解読制限と前記時変鍵とに基づいて前記コンテンツ鍵を生成する、請求項28記載の復号化装置。

【請求項33】 前記前記復号化装置は、前記復号化装置の出入力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、

前記時変鍵生成手段は、前記第1および第2乱数と前記データ系列鍵とに基づいて前記時変鍵を生成する、請求項28記載の復号化装置。

【請求項34】 前記復号化装置は、前記復号化装置の出入力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、

前記時変鍵生成手段は、前記第1および第2乱数と前記共通鍵と前記データ系列鍵とに基づいて前記時変鍵を生成する、請求項28記載の復号化装置。

【請求項35】 前記復号化装置は、前記復号化装置の出入力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、

前記コンテンツ鍵生成手段は、前記第2解読制限と前記データ系列鍵とに基づいて前記コンテンツ生成鍵を生成す

る、請求項28記載の復号化装置。

【請求項36】 前記復号化装置は、前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記コンテンツ鍵生成手段は、前記第2解読制限と前記時変鍵と前記データ系列鍵とに基づいて前記コンテンツ生成鍵を生成する、請求項28記載の復号化装置。

【請求項37】 コンテンツ鍵を用いて暗号化装置と暗号通信を行う手段としてコンピュータを機能させるためのプログラムを記録した記録媒体であって、前記プログラムは、第2解読制限から前記コンテンツ鍵を生成するコンテンツ鍵生成手段、暗号化コンテンツを前記コンテンツ鍵生成手段により生成された前記コンテンツ鍵を用いて復号化する第1復号化手段、として前記コンピュータを機能させる記録媒体。

【請求項38】 前記プログラムは、前記第1解読制限を解読制限更新則に基づいて前記第2解読制限に更新する解読制限更新手段、前記第2解読制限を時変鍵に基づいて暗号化し、第1暗号化解読制限を出力する暗号化手段、として前記コンピュータをさらに機能させる、請求項37記載の記録媒体。

【請求項39】 前記プログラムは、前記共通鍵を記憶する共通鍵記憶手段、前記第2乱数を生成する乱数発生手段、前記第2乱数と第1乱数とを用いて前記暗号化装置と相互認証を行なう相互認証処理手段、前記相互認証処理手段における認証受理をうけて前記第2乱数と前記第1乱数とから前記時変鍵を生成する時変鍵生成手段、第1暗号化解読制限を前記時変鍵を用いて復号化する第2復号化手段、として前記コンピュータをさらに機能させる、請求項38記載の記録媒体。

【請求項40】 前記プログラムは、前記第1解読制限を解読制限更新則に基づいて第2解読制限に更新する解読制限更新手段として前記コンピュータをさらに機能させ、前記コンテンツ鍵生成手段は、前記解読制限更新手段により更新された前記第2解読制限に基づいて前記コンテンツ鍵を生成する、請求項37記載の記録媒体。

【請求項41】 前記プログラムは、前記共通鍵を記憶する第2共通鍵記憶手段、前記第2乱数を生成する第2乱数発生手段、前記第2乱数と第1乱数とを用いて前記暗号化装置と相互認証を行なう相互認証処理手段、前記相互認証処理手段における認証受理をうけて前記第2乱数と前記第1乱数とから前記時変鍵を生成する時変鍵生成手段、暗号化解読制限を前記時変鍵を用いて復号化する第2復

号化手段、として前記コンピュータをさらに機能させる、請求項40記載の記録媒体。

【請求項42】 前記時変鍵生成手段は、前記第1および第2乱数と前記共通鍵に基づいて前記時変鍵を生成する、請求項39記載の記録媒体。

【請求項43】 前記コンテンツ鍵生成手段は、前記第2解読制限と前記時変鍵とに基づいて前記コンテンツ鍵を生成する、請求項39記載の記録媒体。

【請求項44】 前記プログラムは、前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段として前記コンピュータをさらに機能させ、前記時変鍵生成手段は、前記第1および第2乱数と前記データ系列鍵とに基づいて前記時変鍵を生成する、請求項39記載の記録媒体。

【請求項45】 前記プログラムは、前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段として前記コンピュータをさらに機能させ、前記時変鍵生成手段は、前記第1および第2乱数と前記共通鍵と前記データ系列鍵とに基づいて前記時変鍵を生成する、請求項39記載の記録媒体。

【請求項46】 前記プログラムは、前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段として前記コンピュータをさらに機能させ、前記コンテンツ鍵生成手段は、前記第2解読制限と前記データ系列鍵に基づいて前記コンテンツ生成鍵を生成する、請求項39記載の記録媒体。

【請求項47】 前記プログラムは、前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段として前記コンピュータをさらに機能させ、前記コンテンツ鍵生成手段は、前記第2解読制限と前記時変鍵と前記データ系列鍵とに基づいて前記コンテンツ生成鍵を生成する、請求項39記載の記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、解読制限を持った音楽、画像、映像、ゲームなどのデジタルコンテンツを機器間で共通鍵を共有化して暗号通信を行う通信システムにおいて、解読制限の更新が不正に行われた場合に解読できないようにしたものであり、共通鍵に解読制限の更新情報を関連させることによって著作物を保護する著作物保護システム、暗号化装置、復号化装置および記録媒体に関する。

【0002】

【従来の技術】 近年、デジタル情報圧縮技術の進展とインターネットに代表されるグローバルな通信インフラの爆発的な普及によって音楽、画像、映像、ゲームなど

のコンテンツをディジタル情報として通信回線を利用して各家庭に配信することが実現されはじめた。

【0003】通信回線を利用したディジタル情報の配信サービスは、媒体によらないデータだけの流通形態であるため、配信サービス形態の自由度が飛躍的に向上し、単にコンテンツ情報を配信するだけでなく、使用回数、使用期間などの使用制限付きで配信させるなど、多用な形態で流通させることが可能である。

【0004】ディジタルコンテンツの著作権者の権利や流通業者の利益を保護した流通配信システムを確立するために、通信の傍受、盜聴、なりすましなどによる不正入手や、受信したデータを記憶した記録媒体における違法複製、違法改ざんなどの不正行為を防止することが課題となり、正規システムの判別、データスクランブルを行なう暗号／認証などの著作物保護技術が必要となる。

【0005】著作物保護技術については従来より種々なものが知られており、代表的なものとしてデータの暗号化装置と復号化装置間で乱数、応答値の交換を行ない相互に正当性を認証し合い、正当である場合のみデータを送信するチャレンジレスポンス型の相互認証技術がある。

【0006】本明細書において「解読制限」とは、暗号化装置から復号化装置に転送されたコンテンツを使用（再生して音をだすとか）してよいかの情報を意味する。例えば、再生回数付きのコンテンツの場合、解読制限は回数情報である。

【0007】「解読制限の更新」とは、解読制限の更新則を意味する。例えば、再生回数付きのコンテンツの場合、暗号化装置から復号化装置に転送される解読制限（N回使用可能）の回数情報を1つ減らすことを意味する。

【0008】「解読制限の更新情報」とは、更新された解読制限を意味する。例えば、再生回数付きのコンテンツの場合、暗号化装置から復号化装置に転送される解読制限（N回使用可能）が、解読制限の更新によって、解読制限の回数情報が「N-1回使用可能」と書きかえられた情報をさす。

【0009】特に解読制限を持ったディジタルコンテンツを、前述の相互認証技術を用いて暗号通信を行なうシステムを考えた場合、暗号化装置と復号化装置間で相互に正当性を認証し合い、正当であると確認された時のみ解読制限を暗号化装置から復号化装置に暗号通信で転送し、復号化装置は解読制限を解釈して解読可能であるかを判定するとともに解読制限を更新し、更新された解読制限の更新情報を暗号化装置に暗号通信で送信したのち、コンテンツを暗号化装置から暗号通信で復号化装置へロードし、ロードされたコンテンツを解読して使用するのが一般的に行なわれる方法である。

【0010】

【発明が解決しようとする課題】ここで課題となるの

は、解読制限の更新が正常に行なわれること、即ち復号化装置によって更新された解読制限の更新情報が正規の暗号化装置によって受け取られることである。解読制限の更新が正常に行なわれていないと、即ち、復号化装置によって更新された解読制限の更新情報が正規の暗号化装置によって受け取られず、その代わりに正規の暗号化装置になりすました別の偽者の暗号化装置によって受け取られると、正規の暗号化装置で解読制限が更新されることなく正規の暗号化装置からロードされたコンテンツが復号化装置によって解読されるという不正行為が成立する。従って、復号化装置によって更新された解読制限の更新情報が正規の暗号化装置によって受け取られず、その代わりに正規の暗号化装置になりました別の偽者の暗号化装置によって受け取られた場合には、正規の暗号化装置からロードされたコンテンツを復号化装置が解読することができないシステムが必要となる。

【0011】前述の相互認証技術では、通信する機器が正規なものかを判定するだけであり、解読制限の更新が正常に行なわれたかを判定し、不正行為を防止することができない。即ち、解読制限の更新情報を正規の暗号化装置が受け取らず、正規の暗号化装置になりました別の偽者の暗号化装置が受け取った結果、正規の暗号化装置で解読制限が更新されていないにもかかわらず、復号化装置は正規の暗号化装置が送信したコンテンツを不正に解読するという行為を防止することができない。

【0012】本発明の目的は、解読制限の更新を確実に行なうとともに、ディジタルコンテンツの不正解読を防止する著作物保護システム、暗号化装置、復号化装置および記録媒体を提供することにある。

【0013】本発明の他の目的は、復号化装置によって更新された解読制限の更新情報が正規の暗号化装置になりました別の偽者の暗号化装置によって受け取られた場合には、正規の暗号化装置からロードされたコンテンツを復号化装置が解読することができない著作物保護システム、暗号化装置、復号化装置および記録媒体を提供することにある。

【0014】

【課題を解決するための手段】本発明に係る著作物保護システムは、コンテンツ鍵を用いて暗号通信を行う暗号化装置および復号化装置から構成される著作物保護システムであって、前記暗号化装置は、コンテンツを記憶するコンテンツ記憶手段と、第1解読制限を更新して得られる第2解読制限に基づいて前記コンテンツ鍵を生成する第1コンテンツ鍵生成手段と、前記コンテンツを前記コンテンツ鍵に基づいて暗号化し、暗号化コンテンツを出力する第1暗号化手段とを具備し、前記復号化装置は、前記第2解読制限から前記コンテンツ鍵を生成する第2コンテンツ鍵生成手段と、前記暗号化コンテンツを前記第2コンテンツ鍵生成手段により生成された前記コンテンツ鍵を用いて復号化する第1復号化手段とを具備

することを特徴とし、そのことにより上記目的が達成される。

【0015】前記復号化装置は、前記第1解読制限を解読制限更新則に基づいて前記第2解読制限に更新する解読制限更新手段と、前記第2解読制限を時変鍵に基づいて暗号化し、第1暗号化解読制限を出力する第2暗号化手段とをさらに具備し、前記暗号化装置は、前記第2暗号化手段から転送される前記第1暗号化解読制限を前記時変鍵に基づいて復号化し、前記第2解読制限を生成する第2復号化手段とをさらに具備し、前記第1コンテンツ鍵生成手段は、前記第2復号化手段により生成された前記第2解読制限に基づいて前記コンテンツ鍵を生成してもよい。

【0016】前記暗号化装置は、共通鍵を記憶する第1共通鍵記憶手段と、前記第1解読制限を記憶する解読制限記憶手段と、第1乱数を生成する第1乱数発生手段と、前記第1乱数と前記復号化装置から転送される第2乱数とを用いて前記復号化装置と相互認証処理を行なう第1相互認証処理手段と、前記第1相互認証処理手段における認証受理をうけて前記第1乱数と前記第2乱数とから前記時変鍵を生成する第1時変鍵生成手段と、前記第1解読制限を前記時変鍵を用いて暗号化して第2暗号化解読制限を出力する第3暗号化手段とをさらに具備し、前記復号化装置は、前記共通鍵を記憶する第2共通鍵記憶手段と、前記第2乱数を生成する第2乱数発生手段と、前記第2乱数と前記第1乱数とを用いて前記暗号化装置と相互認証を行なう第2相互認証処理手段と、前記第2相互認証処理手段における認証受理をうけて前記第2乱数と前記第1乱数とから前記時変鍵を生成する第2時変鍵生成手段と、前記第2暗号化解読制限を前記時変鍵を用いて復号化する第3復号化手段とをさらに具備してもよい。

【0017】前記復号化装置は、前記第1解読制限を解読制限更新則に基づいて第2解読制限に更新する第1解読制限更新手段をさらに具備し、前記第2コンテンツ鍵生成手段は、前記第1解読制限更新手段により更新された前記第2解読制限に基づいて前記コンテンツ鍵を生成し、前記暗号化装置は、前記復号化装置の第1解読制限更新手段における解読制限の更新をうけて、前記第1解読制限を解読制限更新則に従って前記第2解読制限に更新する第2解読制限更新手段をさらに具備し、前記第1コンテンツ鍵生成手段は、前記第2解読制限更新手段により更新された前記第2解読制限に基づいて前記コンテンツ鍵を生成してもよい。

【0018】前記暗号化装置は、前記共通鍵を記憶する第1共通鍵記憶手段と、前記第1解読制限を記憶する解読制限記憶手段と、第1乱数を生成する第1乱数発生手段と、前記第1乱数と前記復号化装置から転送される第2乱数とを用いて前記復号化装置と相互認証を行なう第1相互認証処理手段と、前記第1相互認証処理手段にお

ける認証受理をうけて前記第1乱数と前記第2乱数とから時変鍵を生成する第1時変鍵生成手段と、前記第1解読制限を前記時変鍵を用いて暗号化して暗号化解読制限を出力する第2暗号化手段とをさらに具備し、前記復号化装置は、前記共通鍵を記憶する第2共通鍵記憶手段と、前記第2乱数を生成する第2乱数発生手段と、前記第2乱数と前記第1乱数とを用いて前記暗号化装置と相互認証を行なう第2相互認証処理手段と、前記第2相互認証処理手段における認証受理をうけて前記第2乱数と前記第1乱数とから前記時変鍵を生成する第2時変鍵生成手段と、前記暗号化解読制限を前記時変鍵を用いて復号化する第2復号化手段とをさらに具備し、そのことにより上記目的が達成される。

【0019】前記第2解読制限更新手段は、予め前記第1解読制限を第2解読制限に更新し、前記第2解読制限更新手段は、前記第1コンテンツ鍵生成手段に更新された前記第2解読制限を出力し、前記第1コンテンツ鍵生成手段は、前記第2解読制限から前記コンテンツ鍵を生成し、前記第2解読制限更新手段は、前記第1暗号化手段の処理が開始されたことをうけて、前記解読制限記憶手段に前記第2解読制限を格納してもよい。

【0020】前記第1および第2時変鍵生成手段は、前記第1および第2乱数と前記共通鍵に基づいて前記時変鍵を生成してもよい。

【0021】前記第1および第2コンテンツ鍵生成手段は、前記第2解読制限と前記時変鍵とに基づいて前記コンテンツ鍵を生成してもよい。

【0022】前記暗号化装置および前記復号化装置は、前記暗号化装置および前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成する第1および第2データ系列鍵生成手段をそれぞれさらに具備し、前記第1および第2時変鍵生成手段は、前記第1および第2乱数と前記データ系列鍵とに基づいて前記時変鍵を生成してもよい。

【0023】前記暗号化装置および前記復号化装置は、前記暗号化装置および前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成する第1および第2データ系列鍵生成手段をそれぞれさらに具備し、前記第1および第2時変鍵生成手段は、前記第1および第2乱数と前記共通鍵と前記データ系列鍵とに基づいて前記時変鍵を生成してもよい。

【0024】前記暗号化装置および前記復号化装置は、前記暗号化装置および前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成する第1および第2データ系列鍵生成手段をそれぞれさらに具備し、前記第1および第2コンテンツ鍵生成手段は、前記第2解読制限と前記データ系列鍵とに基づいて前記コンテンツ生成鍵を生成してもよい。

【0025】前記暗号化装置および前記復号化装置は、前記暗号化装置および前記復号化装置の入出力データ系

列に基づいてデータ系列鍵を生成する第1および第2データ系列鍵生成手段をそれぞれさらに具備し、前記第1および第2コンテンツ鍵生成手段は、前記第2解読制限と前記時変鍵と前記データ系列鍵とに基づいて前記コンテンツ生成鍵を生成してもよい。

【0026】前記第1および第2相互認証処理手段は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に相手機器が正当な機器であることを認証してもよい。

【0027】本発明に係る暗号化装置は、コンテンツ鍵を用いて復号化装置と暗号通信を行う暗号化装置であって、前記暗号化装置は、コンテンツを記憶するコンテンツ記憶手段と、第1解読制限を更新して得られる第2解読制限に基づいて前記コンテンツ鍵を生成するコンテンツ鍵生成手段と、前記コンテンツを前記コンテンツ鍵に基づいて暗号化し、暗号化コンテンツを出力する第1暗号化手段とを具備し、そのことにより上記目的が達成される。

【0028】前記暗号化装置は、前記復号化装置から転送される第1暗号化解読制限を時変鍵に基づいて復号化し、前記第2解読制限を生成する復号化手段をさらに具備し、前記コンテンツ鍵生成手段は、前記復号化手段により生成された前記第2解読制限に基づいて前記コンテンツ鍵を生成してもよい。

【0029】前記暗号化装置は、共通鍵を記憶する共通鍵記憶手段と、前記第1解読制限を記憶する解読制限記憶手段と、第1乱数を生成する第1乱数発生手段と、前記第1乱数と前記復号化装置から転送される第2乱数とを用いて前記復号化装置と相互認証処理を行なう相互認証処理手段と、前記相互認証処理手段における認証受理をうけて前記第1乱数と前記第2乱数とから前記時変鍵を生成する時変鍵生成手段と、前記第1解読制限を前記時変鍵を用いて暗号化して第2暗号化解読制限を出力する第2暗号化手段とをさらに具備してもよい。

【0030】前記暗号化装置は、前記復号化装置の解読制限の更新をうけて、前記第1解読制限を解読制限更新則に従って前記第2解読制限に更新する解読制限更新手段をさらに具備し、前記コンテンツ鍵生成手段は、前記解読制限更新手段により更新された前記第2解読制限に基づいて前記コンテンツ鍵を生成してもよい。

【0031】前記暗号化装置は、前記共通鍵を記憶する共通鍵記憶手段と、前記第1解読制限を記憶する解読制限記憶手段と、第1乱数を生成する第1乱数発生手段と、前記第1乱数と前記復号化装置から転送される第2乱数とを用いて前記復号化装置と相互認証を行なう相互認証処理手段と、前記相互認証処理手段における認証受理をうけて前記第1乱数と前記第2乱数とから時変鍵を生成する時変鍵生成手段と、前記第1解読制限を前記時変鍵を用いて暗号化して暗号化解読制限を出力する第2暗号化手段とをさらに具備してもよい。

【0032】前記解読制限更新手段は、予め前記第1解読制限を第2解読制限に更新し、前記解読制限更新手段は、前記コンテンツ鍵生成手段に更新された前記第2解読制限を出し、前記コンテンツ鍵生成手段は、前記第2解読制限から前記コンテンツ鍵を生成し、前記解読制限更新手段は、前記第1暗号化手段の処理が開始されたことをうけて、前記解読制限記憶手段に前記第2解読制限を格納してもよい。

【0033】前記時変鍵生成手段は、前記第1および第2乱数と前記共通鍵に基づいて前記時変鍵を生成してもよい。

【0034】前記コンテンツ鍵生成手段は、前記第2解読制限と前記時変鍵とに基づいて前記コンテンツ鍵を生成してもよい。

【0035】前記暗号化装置は、前記暗号化装置の出入力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記時変鍵生成手段は、前記第1および第2乱数と前記データ系列鍵とに基づいて前記時変鍵を生成してもよい。

【0036】前記暗号化装置は、前記暗号化装置の出入力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記時変鍵生成手段は、前記第1および第2乱数と前記共通鍵と前記データ系列鍵とに基づいて前記時変鍵を生成してもよい。

【0037】前記暗号化装置は、前記暗号化装置の出入力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記コンテンツ鍵生成手段は、前記第2解読制限と前記データ系列鍵とに基づいて前記コンテンツ生成鍵を生成してもよい。

【0038】前記暗号化装置は、前記暗号化装置の出入力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記コンテンツ鍵生成手段は、前記第2解読制限と前記時変鍵と前記データ系列鍵とに基づいて前記コンテンツ生成鍵を生成してもよい。

【0039】本発明に係る復号化装置は、コンテンツ鍵を用いて暗号化装置と暗号通信を行う復号化装置であって、前記復号化装置は、第2解読制限から前記コンテンツ鍵を生成するコンテンツ鍵生成手段と、暗号化コンテンツを前記コンテンツ鍵生成手段により生成された前記コンテンツ鍵を用いて復号化する第1復号化手段とを具備し、そのことにより上記目的が達成される。

【0040】前記復号化装置は、前記第1解読制限を解読制限更新則に基づいて前記第2解読制限に更新する解読制限更新手段と、前記第2解読制限を時変鍵に基づいて暗号化し、第1暗号化解読制限を出力する暗号化手段とを具備してもよい。

【0041】前記復号化装置は、前記共通鍵を記憶する共通鍵記憶手段と、前記第2乱数を生成する乱数発生手段と、前記第2乱数と第1乱数とを用いて前記暗号化装

置と相互認証を行なう相互認証処理手段と、前記相互認証処理手段における認証受理をうけて前記第2乱数と前記第1乱数とから前記時変鍵を生成する時変鍵生成手段と、第1暗号化解読制限を前記時変鍵を用いて復号化する第2復号化手段とを備えてもよい。

【0042】前記復号化装置は、前記第1解読制限を解読制限更新則に基づいて第2解読制限に更新する解読制限更新手段をさらに備え、前記コンテンツ鍵生成手段は、前記解読制限更新手段により更新された前記第2解読制限に基づいて前記コンテンツ鍵を生成してもよい。

【0043】前記復号化装置は、前記共通鍵を記憶する第2共通鍵記憶手段と、前記第2乱数を生成する第2乱数発生手段と、前記第2乱数と第1乱数とを用いて前記暗号化装置と相互認証を行なう相互認証処理手段と、前記相互認証処理手段における認証受理をうけて前記第2乱数と前記第1乱数とから前記時変鍵を生成する時変鍵生成手段と、暗号化解読制限を前記時変鍵を用いて復号化する第2復号化手段とを具備してもよい。

【0044】前記時変鍵生成手段は、前記第1および第2乱数と前記共通鍵に基づいて前記時変鍵を生成してもよい。

【0045】前記コンテンツ鍵生成手段は、前記第2解読制限と前記時変鍵とにに基づいて前記コンテンツ鍵を生成してもよい。

【0046】前記前記復号化装置は、前記復号化装置の出入力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記時変鍵生成手段は、前記第1および第2乱数と前記データ系列鍵とにに基づいて前記時変鍵を生成してもよい。

【0047】前記復号化装置は、前記復号化装置の出入力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記時変鍵生成手段は、前記第1および第2乱数と前記共通鍵と前記データ系列鍵とにに基づいて前記時変鍵を生成してもよい。

【0048】前記復号化装置は、前記復号化装置の出入力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記コンテンツ鍵生成手段は、前記第2解読制限と前記データ系列鍵に基づいて前記コンテンツ生成鍵を生成してもよい。

【0049】前記復号化装置は、前記復号化装置の出入力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段をさらに具備し、前記コンテンツ鍵生成手段は、前記第2解読制限と前記時変鍵と前記データ系列鍵とにに基づいて前記コンテンツ生成鍵を生成してもよい。

【0050】本発明に係る記録媒体は、コンテンツ鍵を用いて暗号化装置と暗号通信を行う手段としてコンピュータを機能させるためのプログラムを記録した記録媒体であって、前記プログラムは、第2解読制限から前記コンテンツ鍵を生成するコンテンツ鍵生成手段、暗号化コ

ンテンツを前記コンテンツ鍵生成手段により生成された前記コンテンツ鍵を用いて復号化する第1復号化手段、として前記コンピュータを機能させ、そのことにより上記目的が達成される。

【0051】前記プログラムは、前記第1解読制限を解読制限更新則に基づいて前記第2解読制限に更新する解読制限更新手段、前記第2解読制限を時変鍵に基づいて暗号化し、第1暗号化解読制限を出力する暗号化手段、として前記コンピュータをさらに機能させてもよい。

【0052】前記プログラムは、前記共通鍵を記憶する共通鍵記憶手段、前記第2乱数を生成する乱数発生手段、前記第2乱数と第1乱数とを用いて前記暗号化装置と相互認証を行なう相互認証処理手段、前記相互認証処理手段における認証受理をうけて前記第2乱数と前記第1乱数とから前記時変鍵を生成する時変鍵生成手段、第1暗号化解読制限を前記時変鍵を用いて復号化する第2復号化手段、として前記コンピュータをさらに機能させてもよい。

【0053】前記プログラムは、前記第1解読制限を解読制限更新則に基づいて第2解読制限に更新する解読制限更新手段として前記コンピュータをさらに機能させ、前記コンテンツ鍵生成手段は、前記解読制限更新手段により更新された前記第2解読制限に基づいて前記コンテンツ鍵を生成してもよい。

【0054】前記プログラムは、前記共通鍵を記憶する第2共通鍵記憶手段、前記第2乱数を生成する第2乱数発生手段、前記第2乱数と第1乱数とを用いて前記暗号化装置と相互認証を行なう相互認証処理手段、前記相互認証処理手段における認証受理をうけて前記第2乱数と前記第1乱数とから前記時変鍵を生成する時変鍵生成手段、暗号化解読制限を前記時変鍵を用いて復号化する第2復号化手段、として前記コンピュータをさらに機能させてもよい。

【0055】前記時変鍵生成手段は、前記第1および第2乱数と前記共通鍵に基づいて前記時変鍵を生成してもよい。

【0056】前記コンテンツ鍵生成手段は、前記第2解読制限と前記時変鍵とにに基づいて前記コンテンツ鍵を生成してもよい。

【0057】前記プログラムは、前記復号化装置の出入力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段として前記コンピュータをさらに機能させ、前記時変鍵生成手段は、前記第1および第2乱数と前記データ系列鍵とにに基づいて前記時変鍵を生成してもよい。

【0058】前記プログラムは、前記復号化装置の出入力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段として前記コンピュータをさらに機能させ、前記時変鍵生成手段は、前記第1および第2乱数と前記共通鍵と前記データ系列鍵とにに基づいて前記時変鍵

を生成してもよい。

【0059】前記プログラムは、前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段として前記コンピュータをさらに機能させ、前記コンテンツ鍵生成手段は、前記第2解読制限と前記データ系列鍵に基づいて前記コンテンツ生成鍵を生成してもよい。

【0060】前記プログラムは、前記復号化装置の入出力データ系列に基づいてデータ系列鍵を生成するデータ系列鍵生成手段として前記コンピュータをさらに機能させ、前記コンテンツ鍵生成手段は、前記第2解読制限と前記時変鍵と前記データ系列鍵に基づいて前記コンテンツ生成鍵を生成してもよい。

【0061】

【発明の実施の形態】以下に本発明の原理と実施の形態を添付の図面を用いて説明する。本発明では、デジタルコンテンツの暗号通信に用いる共通鍵の生成に解読制限を用いる。

【0062】(実施の形態1) 図1は、本発明の実施の形態1における構成図を示し暗号化装置101と復号化装置102が暗号通信を行なうシステム100を示す。

【0063】暗号化装置101は、共通鍵UKを記憶する共通鍵記憶部103と、解読制限を記憶する解読制限記憶部111と、コンテンツCTを記憶するコンテンツ記憶部121と、乱数R1を生成する乱数発生部105と、乱数R1と復号化装置102から転送される乱数R2と共に共通鍵UKとを用いて復号化装置102と相互認証処理を行なう相互認証処理部107と、相互認証処理部107における相互認証処理に応答して乱数R1と乱数R2とから相互認証処理が実行される度に可変な時変鍵VKを生成する時変鍵生成部109と、解読制限S1を時変鍵VKを用いて暗号化して暗号化解読制限S2を出力する暗号化部113と、復号化装置102の暗号化部116から転送される暗号化解読制限S3を時変鍵VKを用いて解読制限S4に復号化し、解読制限記憶部111に書き込む復号化部115と、解読制限S4からコンテンツ鍵CKを生成するコンテンツ鍵生成部117と、コンテンツCTをコンテンツ鍵CKに基づいて暗号化し、暗号化コンテンツS5を出力する暗号化部119とを備える。

【0064】復号化装置102は、共通鍵UKを記憶する共通鍵記憶部104と、乱数R2を生成する乱数発生部106と、乱数R2と乱数R1と共に共通鍵UKとを用いて暗号化装置101と相互認証処理を行なう相互認証処理部108と、相互認証処理部108における相互認証処理に応答して乱数R2と乱数R1とから時変鍵VKを生成する時変鍵生成部110と、暗号化解読制限S2を時変鍵VKを用いて復号化する復号化部114と、復号化部114で復号化した解読制限S1を解読制限更新則に基づいて解読制限S4に更新する解読制限更新部112

と、解読制限S4を時変鍵VKを用いて暗号化し、暗号化解読制限S3を出力する暗号化部116と、解読制限S4からコンテンツ鍵CKを生成するコンテンツ鍵生成部118と、暗号化コンテンツS5をコンテンツ鍵CKを用いて復号化し、コンテンツCTを出力する復号化部120とを備える。

【0065】暗号化装置101、復号化装置102はともに共通鍵記憶部103、104を備え同一の共通化鍵UKを保持する。尚、予め共通化鍵UKは同一共通鍵として共通鍵記憶部103、104に記憶されていてもよいし、作成プロセスにより同一の共通化鍵UKを作成してもよい。

【0066】暗号化装置101は、解読制限S1を記憶する解読制限記憶部111とコンテンツCTを記憶するコンテンツ記憶部121を備える。なお、これら共通鍵記憶部103、解読制限記憶部111、コンテンツ記憶部121は外部から直接アクセスすることができないプロジェクト領域に配置されている。

【0067】図2は、実施の形態1のシステムの処理手順を示すフローチャートである。以下図1および図2を参照して、暗号化装置101と復号化装置102とを含むシステム100の処理手順を説明する。

【0068】暗号化装置101、復号化装置102は、互いに独立に乱数R1、R2を発生する乱数発生部105、106を備え、互いの乱数R1、R2を交換し、乱数R1と共に共通化鍵UKを用いて応答値V1を作成し、乱数R2と共に共通化鍵UKを用いて応答値V2を作成し、応答値V1、V2を交換し、比較することによって相互に相手機器が正当な機器であることを認証するチャレンジレスポンス型の相互認証を相互認証処理部107、108で行なう(S201)。

【0069】相互認証処理部107、108によって相手機器が正当であることを確認する認証確立が成立したか否かが判断される(S202)。認証確立が成立しないと判断された場合には(S202でNO)、処理は終了する。認証確立が成立したと判断された場合には(S202でYES)、時変鍵生成部109、110は互いの乱数R1、R2から相互認証毎に変化する同一の時変鍵VKを生成する(S203)。その後、暗号化装置101内の解読制限記憶部111に格納されている解読制限S1を時変鍵VKを用いて暗号化部113で暗号化して暗号化解読制限S2を復号化装置102に転送する(S204)。

【0070】復号化部114は受信した暗号化解読制限S2と同じく時変鍵VKを用いて復号化する(S205)。復号化部114にて復号化された解読制限S1を解読制限更新部112は解読制限更新則に従って更新し(S206)、更新された解読制限S4を時変鍵VKを用いて暗号化して(S207)暗号化解読制限S3を暗号化装置101に転送する。復号化部115は、転送さ

れた暗号化解読制限S3を時変鍵VKを用いて復号化して更新された解読制限S4を得て、解読制限記憶部111に格納する(S208)。

【0071】コンテンツ鍵生成部117は解読制限S4からコンテンツ鍵CKを生成する(S209)。コンテンツ記憶部121に格納されているコンテンツCTを暗号化装置101から復号化装置102に転送する場合、暗号化部119はコンテンツ鍵CKを用いてコンテンツCTを暗号化する(S210)。コンテンツ鍵生成部118は解読制限S4からコンテンツ鍵CKを生成する(S211)。復号化装置内復号化部120はコンテンツ鍵CKを用いて暗号化コンテンツS5を復号する(S212)。

【0072】なお、本実施の形態では、1回の認証確立後コンテンツを暗号化装置から復号化装置に転送する例を示したが、認証確立後、送復号化装置間でコンテンツ転送が発生する毎に相手機器が正当であることを確認する相互認証を行うようにしてもよい。また、時変鍵VKの生成に、相互認証に用いた乱数R1、R2を用いたが、応答値V1、V2を用いてもかまわない。

【0073】また、解読制限、コンテンツの暗号化および復号化に用いる方法は異なるアルゴリズムでも同一のアルゴリズムのものを用いてよく、例えばDES(Data Encryption Standard)などを用いればよい。

【0074】また、時変鍵、コンテンツ鍵の生成に用いる方法は異なるアルゴリズムでも同一のアルゴリズムのものを用いてよく、例えばSHA(Secure Hash Algorithm)などの一方指向性の関数を用いればよい。

【0075】なお本実施の形態では本発明を分かりやすく説明するために、送受信を相互認証処理部107、108、暗号化部113、復号化部114、復号化部115、暗号化部116、暗号化部119、復号化部120が行っている例を示しているが、実際の送受信は、制御部122、123で管理されることが一般的である。後述する実施の形態でも同様である。

【0076】以上のように、本実施の形態の著作物保護システムは、著作物であるコンテンツCTの転送において、解読制限の更新情報(解読制限S4)を関連させてコンテンツの暗号通信を行うので、正しく解読制限S1の更新処理を行わないと、コンテンツCTを解読できないという効果がある。

【0077】(実施の形態2)図3は、本発明の実施の形態2における著作物保護システム200を示す。図2において図1と同一の構成要素には同一の参照符号を付し、説明を省略する。

【0078】著作物保護システム200では、図1で示した著作物保護システム100のように解読制限更新部112で更新された解読制限S4を暗号化/復号化を行

なって転送し、解読制限記憶部111に格納するのではなく、暗号化装置201内にも解読制限更新部223を備える。

【0079】復号化装置202の解読制限更新部212は、解読制限S1の更新を命令する解読制限更新指令CCだけを解読制限更新部223に転送する。解読制限更新部223は転送された解読制限更新指令CCを受けとり、解読制限S1を更新し、更新した解読制限S4を解読制限記憶部211に格納する。

【0080】以上のように、本実施の形態の著作物保護システム200は、コンテンツ鍵CKの生成に関連する更新された解読制限S4を復号化装置202から暗号化装置201へ転送する必要がないため、解読制限S4の秘匿性を高めることができる。また、更新された解読制限S4の転送に係る暗号化部、復号化部を削除することができるためシステム規模を小さくできるという効果がある。

【0081】(実施の形態3)図4は、本発明の実施の形態3における著作物保護システム300を示す。図3において図1と同一の構成には同一の符号を付し説明を省略する。

【0082】著作物保護システム300では、図2で示した著作物保護システム200のように解読制限更新部212からの更新指令CCをうけて暗号化装置201内の解読制限更新部223によって解読制限S1を更新するのではなく、予め暗号化装置301内の解読制限記憶部311に格納されている解読制限S1を解読制限更新部323によって更新する。コンテンツ鍵生成部117が更新された解読制限S4を用いてコンテンツ鍵CKを生成し、暗号化部319がコンテンツCTの暗号化を開始することに応答して、解読制限更新部323は解読制限記憶部311に更新された解読制限S4を格納する。

【0083】以上のように、本実施の形態の著作物保護システム300は、復号化装置302からの指令で解読制限S1を更新するのではなく、予め解読制限更新部323が解読制限S1を更新し、かつコンテンツ鍵生成部117がデータ転送鍵CKを生成するので、処理ステップを短縮できるという効果がある。

【0084】(実施の形態4)図5は、本発明の実施の形態4における著作権保護システム400を示す。図4において図1と同一の構成には同一の符号を付し説明を省略する。

【0085】著作権保護システム400では、時変鍵生成部409、410における時変鍵VKの生成において、乱数R1、R2に加えて共通鍵UKを用いる。なお、時変鍵VKは、例えば、乱数R1、R2、共通鍵UKを排他的論理和で結合し、一方指向性関数による変換を行なって生成すればよい。

【0086】以上のように、本実施の形態の著作権保護システム400によれば、外部でモニタ可能な乱数R

1、R₂だけから時変鍵VKを生成するのではなく、秘密な共通鍵UKを関連付けるようにして時変鍵VKを生成しているので時変鍵VKの類推が容易でなく、時変鍵VKの秘匿性を向上させることができるという効果がある。

【0087】(実施の形態5)図6は、本発明の実施の形態5における著作権保護システム500を示す。図5において図1と同一の構成には同一の符号を付し説明を省略する。

【0088】著作権保護システム500では、コンテンツ鍵生成部517、518におけるコンテンツ鍵CKの生成において、更新された解読制限S4に加えて時変鍵VKを用いる。なお、コンテンツ鍵CKは、例えば、解読制限S4、時変鍵VKを排他的論理和で結合し、一方向性関数による変換を行なって生成すればよい。

【0089】以上のように、本実施の形態の著作権保護システム500によれば、更新された解読制限S4だけから時変鍵CKを生成するのではなく、相互認証毎に時系列的に変化する時変鍵VKを関連付けるようにし、時変鍵CKを生成しているので、よりコンテンツの暗号化の強度を向上させることができるという効果がある。

【0090】(実施の形態6)図7は、本発明の実施の形態6における著作権保護システム600を示す。図6において図1と同一の構成には同一の符号を付し説明を省略する。

【0091】著作物保護システム600では、暗号化装置601および復号化装置602に入力または出力される入出力データの全体または一部(ここでは、乱数R1、R2、応答値V1、V2、暗号化解読制限S2、S3、暗号化コンテンツS5)からデータ系列鍵TK1を生成するデータ系列鍵生成部625、626を暗号化装置601および復号化装置602に備える。時変鍵生成部609、610およびコンテンツ鍵生成部617、618における鍵の生成にデータ系列鍵TK1を加える。

【0092】なお、データ系列鍵TK1は、例えば、各入出力データのHighまたはLowをカウントして生成すればよい。また、時変鍵VKは、例えば、乱数R1、R2、データ系列鍵TK1を排他的論理和で結合し、一方向性関数による変換を行なって生成すればよい。また、コンテンツ鍵CKは、解読制限S4、データ系列鍵TK1を排他的論理和で結合し、一方向性関数による変換を行なって生成すればよい。また、入出力される入出力データの全てからデータ系列鍵TK1を生成する必要はなく、そのうちの一部から生成するようにもかまわない。

【0093】以上のように、本実施の形態の著作権保護システム600は、暗号化装置および復号化装置に入出力される入出力データを監視し、入出力データから各装置に共通なデータ系列鍵TK1を生成し、生成されたデータ系列鍵TK1を各コンテンツ鍵の生成に関連付ける

ようしている。暗号通信の対象となる暗号化装置と復号化装置との間で入出力データが同一である必要があるため、通信のなりすましを防止することができるという効果がある。

【0094】(実施の形態7)図8は、本発明の実施の形態7における構成図を示し暗号化装置101と復号化装置102が暗号通信を行なうシステム800を示す。図8を参照して、暗号化装置および復号化装置が直接接続されて使用される様子を説明する。実施の形態1で前述した構成要素と同一の構成要素には同一の参照符号を付している。これらの構成要素についての詳細な説明は省略する。

【0095】システム800は、コンテンツを再生するコンテンツ再生装置801とコンテンツ再生装置801に装着された実施の形態1で前述した暗号化装置101とを含む。コンテンツ再生装置801は、実施の形態1で前述した復号化装置102と復号化装置102によって復号されたコンテンツを再生する再生部802とを含む。

【0096】このように、実施の形態1で前述した復号化装置102は、コンテンツを再生するコンテンツ再生装置801に含まれ得る。実施の形態1で前述した暗号化装置101は、コンテンツ再生装置801に装着して使用される。コンテンツ再生装置801に装着された暗号化装置101とコンテンツ再生装置801に含まれる復号化装置102とは、実施の形態1で前述したように暗号通信を行なう。

【0097】コンテンツ再生装置801は、携帯電話であり得る。コンテンツ再生装置801はオーディオプレーヤーであってもよく、パーソナルコンピュータであってもよい。暗号化装置101は、メモリカードであり得る。暗号化装置101は、実施の形態2～6で前述した暗号化装置201～601のいずれかであってもよく、復号化装置102は、実施の形態2～6で前述した復号化装置202～602のいずれかであってもよいことは、言うまでもない。

【0098】復号化装置102は、実施の形態1～6で前述したように復号化装置を動作させるためのプログラムを記録した記録媒体803から読み出したプログラムにより動作し得る。記録媒体803は、CD-ROMであり得る。

【0099】図9は、本発明の実施の形態7における他の構成図を示し暗号化装置101と復号化装置102が暗号通信を行なうシステム800を示す。図8を参照して、暗号化装置および復号化装置が電気通信回線により接続されて使用される様子を説明する。実施の形態1および実施の形態7の図8で前述した構成要素と同一の構成要素には同一の参照符号を付している。これらの構成要素についての詳細な説明は省略する。

【0100】図9を参照して、システム900は、コン

テツを再生するコンテンツ再生装置801と、サーバ901と、コンテンツ再生装置801とサーバ901とを接続する電気通信回線903とを含む。コンテンツ再生装置801は、実施の形態1で前述した復号化装置102と復号化装置102によって復号されたコンテンツを再生する再生部802とを含む。サーバ901は、サーバ901に装着された実施の形態1で前述した暗号化装置101を含む。

【0101】このようにコンテンツを再生するコンテンツ再生装置801とサーバ901とは、電気通信回線903を介して接続されている。暗号化装置101は、サーバ901に装着して使用される。サーバ901に装着された暗号化装置101とコンテンツ再生装置801に含まれる復号化装置102とは、電気通信回線903を介して実施の形態1で前述したように暗号通信を行なう。

【0102】電気通信回線903は、インターネットであり得る。電気通信回線903は、ローカルエリアネットワーク(LAN)であってもよい。

【0103】図8で示した態様と同様に、コンテンツ再生装置801は、携帯電話であり得る。コンテンツ再生装置801はオーディオプレーヤーであってもよく、パソコン用コンピュータであってもよい。暗号化装置101は、メモリカードであり得る。暗号化装置101は、実施の形態2～6で前述した暗号化装置201～601のいずれかであってもよく、復号化装置102は、実施の形態2～6で前述した復号化装置202～602のいずれかであってもよいことは、言うまでもない。

【0104】図8で示した態様と同様に、復号化装置102は、復号化装置102を実施の形態1～6で前述したように動作させるためのプログラムを記録した記録媒体803から読み出したプログラムにより動作し得る。

【0105】図9では暗号化装置101および復号化装置102が電気通信回線903を介して接続されて使用される態様を説明したが、本発明はこれに限定されない。暗号化装置101および復号化装置102は、無線通信回線を介して接続されていてもよい。

【0106】

【発明の効果】以上のように本発明によれば、解読制限の更新を確実に行なうとともに、ディジタルコンテンツの不正解読を防止する著作物保護システム、暗号化装置、復号化装置および記録媒体を提供することができる。

【0107】また本発明によれば、復号化装置によって更新された解読制限の更新情報が正規の暗号化装置になりました別の偽者の暗号化装置によって受け取られた場合には、正規の暗号化装置からロードされたコンテンツを復号化装置が解読することができない著作物保護システム、暗号化装置、復号化装置および記録媒体を提供することができる。

【0108】さらに本発明によれば、著作物であるコンテンツの転送において、解読制限の更新情報を関連させて暗号通信を行うので、正しく解読制限の更新処理を行わないと、コンテンツを解読できないという効果を奏する著作物保護システム、暗号化装置、復号化装置および記録媒体を提供することができる。

【0109】さらに本発明によれば、データ転送鍵の生成に関連する更新された解読制限を復号化装置から暗号化装置へ転送しなくても良いため、解読制限の秘匿性を高めることができ、また、更新された解読制限の転送に係わる暗号化部、復号化部を削除することができるためシステム規模を小さくできるという効果を奏する著作物保護システム、暗号化装置、復号化装置および記録媒体を提供することができる。

【0110】さらに本発明によれば、復号化装置からの指令で解読制限を更新するのではなく、予め暗号化装置が解読制限を更新し、かつデータ転送鍵を生成しているので、処理ステップを短縮できるという効果を奏する著作物保護システム、暗号化装置、復号化装置および記録媒体を提供することができる。

【0111】さらに本発明によれば、外部でモニタ可能な乱数だけから時変鍵を生成するのではなく、秘密な共通鍵を関連付けるように時変鍵を生成しているので時変鍵の類推が容易でなく、時変鍵の秘匿性を向上させることができるという効果を奏する著作物保護システム、暗号化装置、復号化装置および記録媒体を提供することができる。

【0112】さらに本発明によれば、暗号化装置および復号化装置に入出力される入出力データを監視し、入出力データから各装置に共通なデータ系列鍵を生成し、生成されたデータ系列鍵を各コンテンツ鍵の生成に関連付けるようにしているので、通信のなりすましを防止することができるという効果を奏する著作物保護システム、暗号化装置、復号化装置および記録媒体を提供することができる。

【図面の簡単な説明】

【図1】実施の形態1に係るシステムの構成を示す構成図である。

【図2】実施の形態1に係るシステムの処理手順を示すフローチャートである。

【図3】実施の形態2に係るシステムの構成を示す構成図である。

【図4】実施の形態3に係るシステムの構成を示す構成図である。

【図5】実施の形態4に係るシステムの構成を示す構成図である。

【図6】実施の形態5に係るシステムの構成を示す構成図である。

【図7】実施の形態6に係るシステムの構成を示す構成図である。

【図8】実施の形態7に係るシステムの構成を示す構成図である。

【図9】実施の形態7に係るシステムの他の構成を示す構成図である。

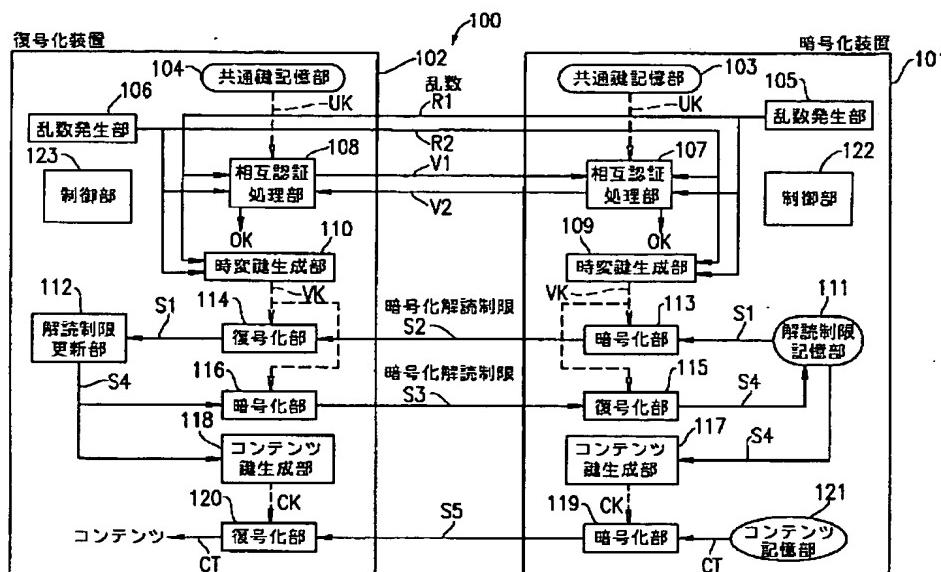
【符号の説明】

101、201、301、401、501、601
暗号化装置

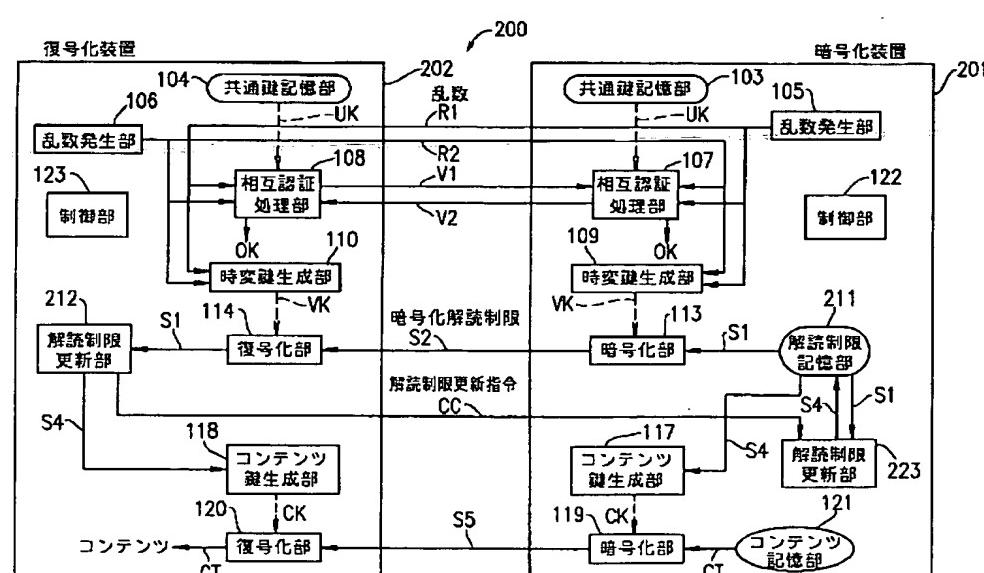
102、202、302、402、502、602
復号化装置

103、104 共通鍵記憶部
105、106 亂数発生部
107、108 相互認証処理部
109、110、609、610 時変鍵生成部
111、211、311 解読制限記憶部
112、212、223、323 解析制限更新部
113、116、119 暗号化部
114、115、120 復号化部
117、118、617、618 コンテンツ鍵生成部
119、120 CK CT
121、122 制御部
123 S1 S4
124 S2 S3
125 S4 S4
126 S5
127 S1
128 S1
129 S1
130 S1
131 S1
132 S1
133 S1
134 S1
135 S1
136 S1
137 S1
138 S1
139 S1
140 S1
141 S1
142 S1
143 S1
144 S1
145 S1
146 S1
147 S1
148 S1
149 S1
150 S1
151 S1
152 S1
153 S1
154 S1
155 S1
156 S1
157 S1
158 S1
159 S1
160 S1
161 S1
162 S1
163 S1
164 S1
165 S1
166 S1
167 S1
168 S1
169 S1
170 S1
171 S1
172 S1
173 S1
174 S1
175 S1
176 S1
177 S1
178 S1
179 S1
180 S1
181 S1
182 S1
183 S1
184 S1
185 S1
186 S1
187 S1
188 S1
189 S1
190 S1
191 S1
192 S1
193 S1
194 S1
195 S1
196 S1
197 S1
198 S1
199 S1
200 S1
201 S1
202 S1
203 S1
204 S1
205 S1
206 S1
207 S1
208 S1
209 S1
210 S1
211 S1
212 S1
213 S1
214 S1
215 S1
216 S1
217 S1
218 S1
219 S1
220 S1
221 S1
222 S1
223 S1
224 S1
225 S1
226 S1
227 S1
228 S1
229 S1
230 S1
231 S1
232 S1
233 S1
234 S1
235 S1
236 S1
237 S1
238 S1
239 S1
240 S1
241 S1
242 S1
243 S1
244 S1
245 S1
246 S1
247 S1
248 S1
249 S1
250 S1
251 S1
252 S1
253 S1
254 S1
255 S1
256 S1
257 S1
258 S1
259 S1
260 S1
261 S1
262 S1
263 S1
264 S1
265 S1
266 S1
267 S1
268 S1
269 S1
270 S1
271 S1
272 S1
273 S1
274 S1
275 S1
276 S1
277 S1
278 S1
279 S1
280 S1
281 S1
282 S1
283 S1
284 S1
285 S1
286 S1
287 S1
288 S1
289 S1
290 S1
291 S1
292 S1
293 S1
294 S1
295 S1
296 S1
297 S1
298 S1
299 S1
300 S1
301 S1
302 S1
303 S1
304 S1
305 S1
306 S1
307 S1
308 S1
309 S1
310 S1
311 S1
312 S1
313 S1
314 S1
315 S1
316 S1
317 S1
318 S1
319 S1
320 S1
321 S1
322 S1
323 S1
324 S1
325 S1
326 S1
327 S1
328 S1
329 S1
330 S1
331 S1
332 S1
333 S1
334 S1
335 S1
336 S1
337 S1
338 S1
339 S1
340 S1
341 S1
342 S1
343 S1
344 S1
345 S1
346 S1
347 S1
348 S1
349 S1
350 S1
351 S1
352 S1
353 S1
354 S1
355 S1
356 S1
357 S1
358 S1
359 S1
360 S1
361 S1
362 S1
363 S1
364 S1
365 S1
366 S1
367 S1
368 S1
369 S1
370 S1
371 S1
372 S1
373 S1
374 S1
375 S1
376 S1
377 S1
378 S1
379 S1
380 S1
381 S1
382 S1
383 S1
384 S1
385 S1
386 S1
387 S1
388 S1
389 S1
390 S1
391 S1
392 S1
393 S1
394 S1
395 S1
396 S1
397 S1
398 S1
399 S1
400 S1
401 S1
402 S1
403 S1
404 S1
405 S1
406 S1
407 S1
408 S1
409 S1
410 S1
411 S1
412 S1
413 S1
414 S1
415 S1
416 S1
417 S1
418 S1
419 S1
420 S1
421 S1
422 S1
423 S1
424 S1
425 S1
426 S1
427 S1
428 S1
429 S1
430 S1
431 S1
432 S1
433 S1
434 S1
435 S1
436 S1
437 S1
438 S1
439 S1
440 S1
441 S1
442 S1
443 S1
444 S1
445 S1
446 S1
447 S1
448 S1
449 S1
450 S1
451 S1
452 S1
453 S1
454 S1
455 S1
456 S1
457 S1
458 S1
459 S1
460 S1
461 S1
462 S1
463 S1
464 S1
465 S1
466 S1
467 S1
468 S1
469 S1
470 S1
471 S1
472 S1
473 S1
474 S1
475 S1
476 S1
477 S1
478 S1
479 S1
480 S1
481 S1
482 S1
483 S1
484 S1
485 S1
486 S1
487 S1
488 S1
489 S1
490 S1
491 S1
492 S1
493 S1
494 S1
495 S1
496 S1
497 S1
498 S1
499 S1
500 S1
501 S1
502 S1
503 S1
504 S1
505 S1
506 S1
507 S1
508 S1
509 S1
510 S1
511 S1
512 S1
513 S1
514 S1
515 S1
516 S1
517 S1
518 S1
519 S1
520 S1
521 S1
522 S1
523 S1
524 S1
525 S1
526 S1
527 S1
528 S1
529 S1
530 S1
531 S1
532 S1
533 S1
534 S1
535 S1
536 S1
537 S1
538 S1
539 S1
540 S1
541 S1
542 S1
543 S1
544 S1
545 S1
546 S1
547 S1
548 S1
549 S1
550 S1
551 S1
552 S1
553 S1
554 S1
555 S1
556 S1
557 S1
558 S1
559 S1
560 S1
561 S1
562 S1
563 S1
564 S1
565 S1
566 S1
567 S1
568 S1
569 S1
570 S1
571 S1
572 S1
573 S1
574 S1
575 S1
576 S1
577 S1
578 S1
579 S1
580 S1
581 S1
582 S1
583 S1
584 S1
585 S1
586 S1
587 S1
588 S1
589 S1
590 S1
591 S1
592 S1
593 S1
594 S1
595 S1
596 S1
597 S1
598 S1
599 S1
600 S1
601 S1
602 S1
603 S1
604 S1
605 S1
606 S1
607 S1
608 S1
609 S1
610 S1
611 S1
612 S1
613 S1
614 S1
615 S1
616 S1
617 S1
618 S1
619 S1
620 S1
621 S1
622 S1
623 S1
624 S1
625 S1
626 S1
627 S1
628 S1
629 S1
630 S1
631 S1
632 S1
633 S1
634 S1
635 S1
636 S1
637 S1
638 S1
639 S1
640 S1
641 S1
642 S1
643 S1
644 S1
645 S1
646 S1
647 S1
648 S1
649 S1
650 S1
651 S1
652 S1
653 S1
654 S1
655 S1
656 S1
657 S1
658 S1
659 S1
660 S1
661 S1
662 S1
663 S1
664 S1
665 S1
666 S1
667 S1
668 S1
669 S1
670 S1
671 S1
672 S1
673 S1
674 S1
675 S1
676 S1
677 S1
678 S1
679 S1
680 S1
681 S1
682 S1
683 S1
684 S1
685 S1
686 S1
687 S1
688 S1
689 S1
690 S1
691 S1
692 S1
693 S1
694 S1
695 S1
696 S1
697 S1
698 S1
699 S1
700 S1
701 S1
702 S1
703 S1
704 S1
705 S1
706 S1
707 S1
708 S1
709 S1
710 S1
711 S1
712 S1
713 S1
714 S1
715 S1
716 S1
717 S1
718 S1
719 S1
720 S1
721 S1
722 S1
723 S1
724 S1
725 S1
726 S1
727 S1
728 S1
729 S1
730 S1
731 S1
732 S1
733 S1
734 S1
735 S1
736 S1
737 S1
738 S1
739 S1
740 S1
741 S1
742 S1
743 S1
744 S1
745 S1
746 S1
747 S1
748 S1
749 S1
750 S1
751 S1
752 S1
753 S1
754 S1
755 S1
756 S1
757 S1
758 S1
759 S1
760 S1
761 S1
762 S1
763 S1
764 S1
765 S1
766 S1
767 S1
768 S1
769 S1
770 S1
771 S1
772 S1
773 S1
774 S1
775 S1
776 S1
777 S1
778 S1
779 S1
780 S1
781 S1
782 S1
783 S1
784 S1
785 S1
786 S1
787 S1
788 S1
789 S1
790 S1
791 S1
792 S1
793 S1
794 S1
795 S1
796 S1
797 S1
798 S1
799 S1
800 S1
801 S1
802 S1
803 S1
804 S1
805 S1
806 S1
807 S1
808 S1
809 S1
810 S1
811 S1
812 S1
813 S1
814 S1
815 S1
816 S1
817 S1
818 S1
819 S1
820 S1
821 S1
822 S1
823 S1
824 S1
825 S1
826 S1
827 S1
828 S1
829 S1
830 S1
831 S1
832 S1
833 S1
834 S1
835 S1
836 S1
837 S1
838 S1
839 S1
840 S1
841 S1
842 S1
843 S1
844 S1
845 S1
846 S1
847 S1
848 S1
849 S1
850 S1
851 S1
852 S1
853 S1
854 S1
855 S1
856 S1
857 S1
858 S1
859 S1
860 S1
861 S1
862 S1
863 S1
864 S1
865 S1
866 S1
867 S1
868 S1
869 S1
870 S1
871 S1
872 S1
873 S1
874 S1
875 S1
876 S1
877 S1
878 S1
879 S1
880 S1
881 S1
882 S1
883 S1
884 S1
885 S1
886 S1
887 S1
888 S1
889 S1
890 S1
891 S1
892 S1
893 S1
894 S1
895 S1
896 S1
897 S1
898 S1
899 S1
900 S1
901 S1
902 S1
903 S1
904 S1
905 S1
906 S1
907 S1
908 S1
909 S1
910 S1
911 S1
912 S1
913 S1
914 S1
915 S1
916 S1
917 S1
918 S1
919 S1
920 S1
921 S1
922 S1
923 S1
924 S1
925 S1
926 S1
927 S1
928 S1
929 S1
930 S1
931 S1
932 S1
933 S1
934 S1
935 S1
936 S1
937 S1
938 S1
939 S1
940 S1
941 S1
942 S1
943 S1
944 S1
945 S1
946 S1
947 S1
948 S1
949 S1
950 S1
951 S1
952 S1
953 S1
954 S1
955 S1
956 S1
957 S1
958 S1
959 S1
960 S1
961 S1
962 S1
963 S1
964 S1
965 S1
966 S1
967 S1
968 S1
969 S1
970 S1
971 S1
972 S1
973 S1
974 S1
975 S1
976 S1
977 S1
978 S1
979 S1
980 S1
981 S1
982 S1
983 S1
984 S1
985 S1
986 S1
987 S1
988 S1
989 S1
990 S1
991 S1
992 S1
993 S1
994 S1
995 S1
996 S1
997 S1
998 S1
999 S1
1000 S1

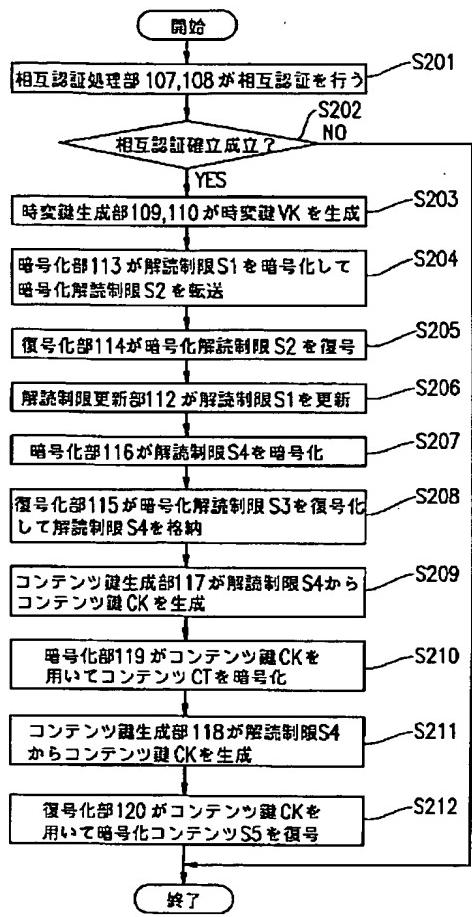
【図1】



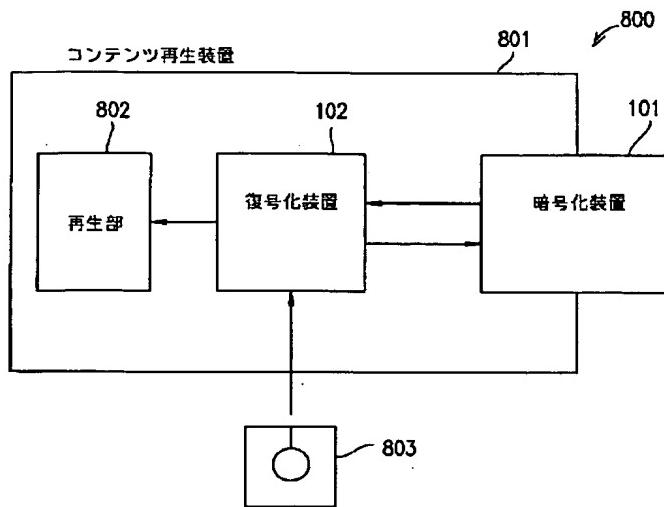
【図3】



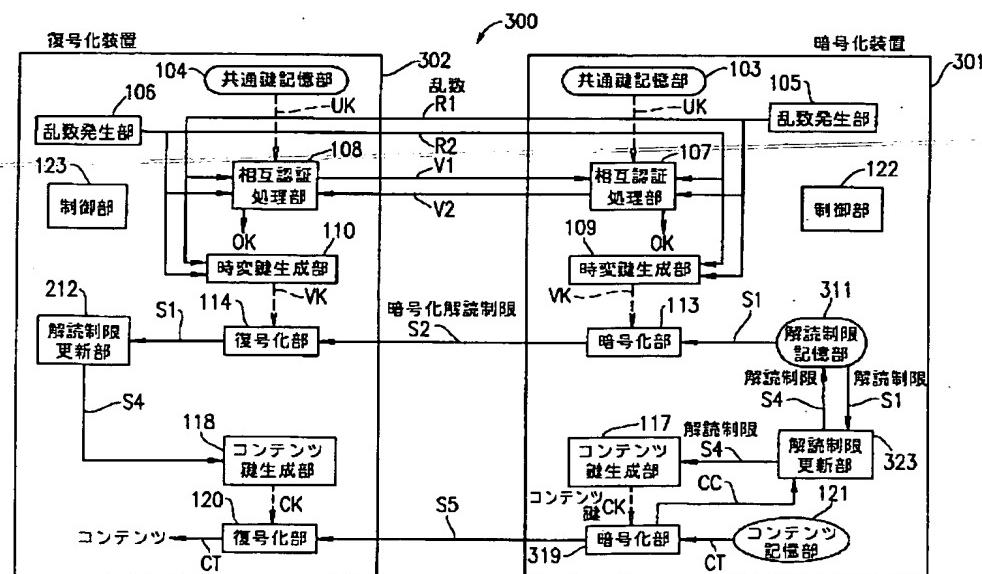
【図2】



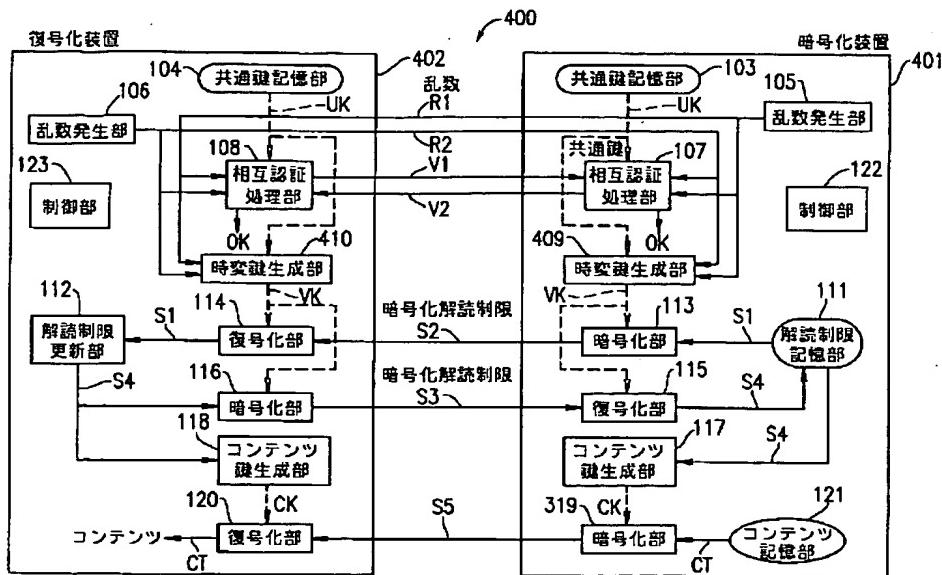
【図8】



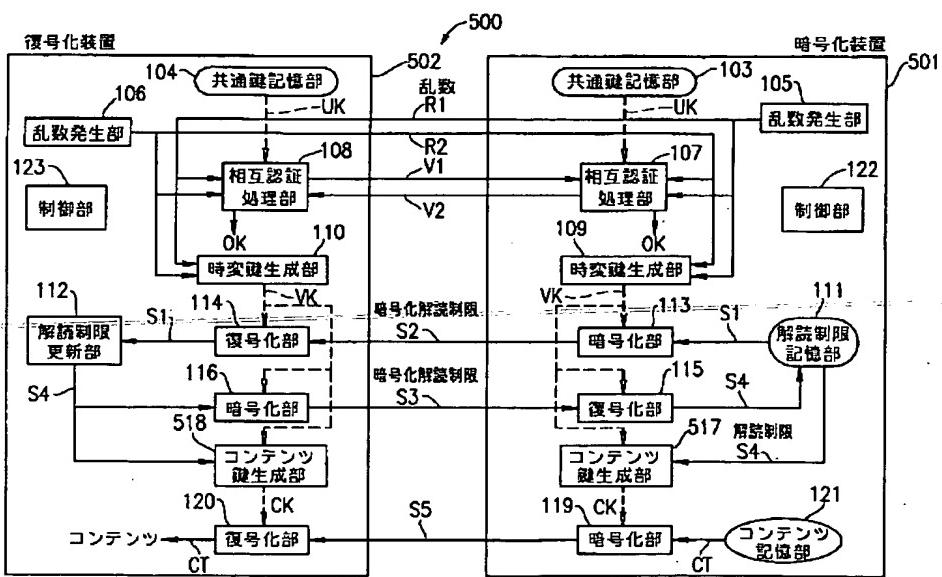
【図4】



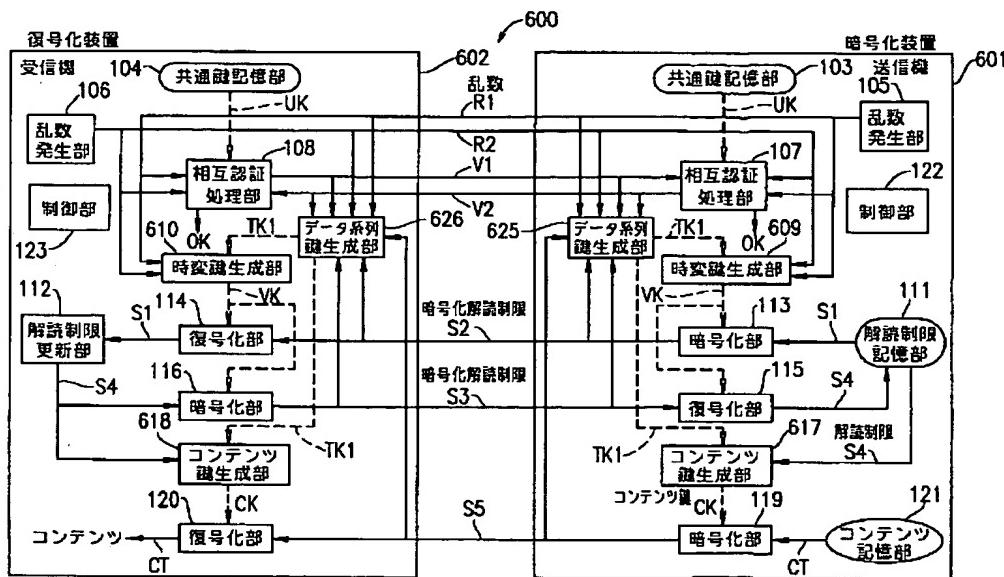
【図5】



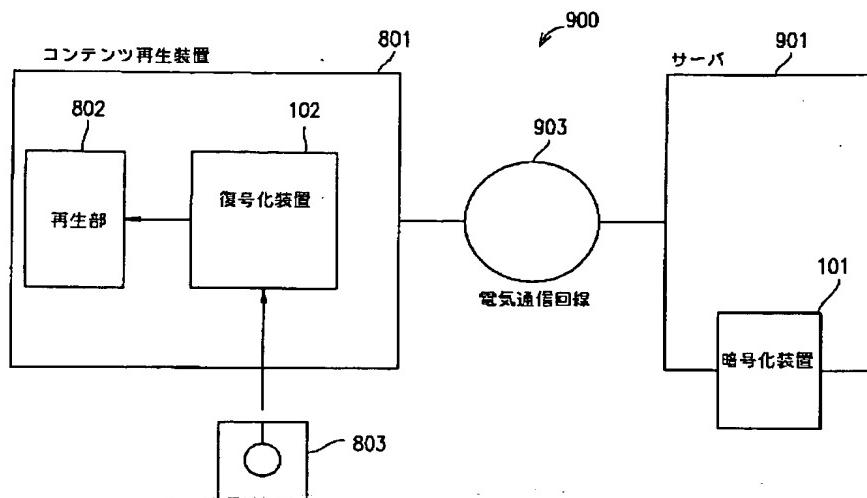
【図6】



【図7】



【図9】



フロントページの続き

(51) Int.CI.7
G 0 6 F 17/60識別記号
3 0 2
5 1 2F I
G 0 6 F 17/60
H 0 4 L 9/00テマコード (参考)
5 1 2
6 0 1 B
6 0 1 E

Fターム(参考) 5B017 AA03 AA07 BA07 BB10 CA15
CA16
5B082 EA11 GA11
5J104 AA01 AA13 AA16 EA01 EA04
EA18 JA03 NA02